Finite degree Galois extensions without finite Galois groups

by Wolter Willemsen

Mathematical Institute, University of Utrecht, the Netherlands

Communicated by Prof. T.A. Springer at the meeting of May 30, 1983

INTRODUCTION

Let L/K be a finite degree Galois extension of skew fields. A group G of automorphisms of L is said to be a Galois group of L/K if K is the fixed field of G. L/K may have many different Galois groups and the question arises whether it has finite ones. Uwe Albrecht gave a criterion for L/K not to admit any finite Galois groups ([1], Satz 2). This criterion is confined to the case that K is the center of L. In this paper we give a generalization without this restriction.

NOTATIONS

We use the following notations for skew fields $K \subseteq L$, $x \in L$, and G a group of automorphisms of L.

$C_L(K)$: the centralizer of K in L.
$C(L)$: the center of L.
$G(L/K)$: the group of all K-automorphisms of L.
int (x) : the inner automorphism mapping y to xyx^{-1}.
$I(G)$: the group consisting of all inner automorphisms of L which are contained in G.
$F(G)$: the fixed field of G in L.

DEFINITION 1. ([1], def. 1) A natural number n has property P if and only if for any group G of order n there are an ordered sequence $(p_1, \ldots, p_k)$ of prime numbers and an ordered sequence $(r_1, \ldots, r_k)$ of natural numbers with $n = \prod_{i=1}^{k} p_i^{r_i}$, such that $G_1 = G$ has a normal p_1 – Sylow group H_1, $G_2 = G_1/H_1$ has a normal p_2 – Sylow group H_2, and so on.

THEOREM. *Let L/K be a skew field extension of finite left degree n satisfying the following conditions:*

1. *$C_L(K)$ is not commutative.*
2. *char (K) does not divide n.*
3. *If p is a prime number and $C_L(K)$ contains a primitive p-th root of unity, then p is less than all prime divisors of n.*
4. *The number n has property P.*

Then L/K does not admit any finite Galois groups.

REMARK. One obtains Albrecht's original theorem by substituting $C(L)$ for K.

For the proof of the theorem it is convenient to have a slight modification of definition 1:

DEFINITION 2. Let $(p_1, \ldots, p_k)$ be an ordered sequence of prime numbers. A group has property $P(p_1, \ldots, p_k)$ if there are nonnegative integers $r_1, \ldots, r_k$ with $\# G = \prod_{i=1}^{k} p_i^{r_i}$, $G_1 = G$ has a normal p_1 – Sylow group H_1, $G_2 = G_1/H_1$ has a normal p_2 – Sylow group H_2, and so on.

LEMMA. *Let $p_1, \ldots, p_k$ be prime numbers. If a group G has property $P(p_1, \ldots, p_k)$, then every subgroup of G and every factor group of G have this property.*

The proof of this lemma is straightforward.

PROOF OF THE THEOREM. Suppose L/K has a finite Galois group G of order g. Let p be a prime divisor of g. Let G' be a subgroup of G of order p. Then $1 < [L : F(G')] \leq p$. $[L : F(G')]$ divides n, so $p \geq q$, where q is the least prime divisor of n. By the third hypothesis, $C_L(K)$ does not contain a primitive p-th root of unity. Let G_p be a p – Sylow group of G. Because $C(F(G_p)) \subset C_L(k)$ we can apply [3, Satz 4]: $[L : F(G_p)]$ divides $\# G_p$. $L \neq F(G_p)$, so p divides $[L : F(G_p)]$, which in turn divides n; so by the second hypothesis $p \neq \text{char}\,(K)$. Therefore, again by [3, Satz 4], $[L : F(G_p)] = \# G_p$; so $\# G_p$ divides n, for all prime divisors p of g. Thus we find that g divides n and therefore $g = n$. Now every K-automorphism of L leaves $C_L(K)$ invariant as a whole. In particular, $I(G)$ induces a group H of automorphisms of $C_L(K)$. Since G is a Galois group of L/K it follows from [3, Satz 2] that $I(G)$ contains a subset $\{\text{int}\,(x) | x \in B\}$ where B is a $C(L)$ – basis of $C_L(K)$. Now $F(I(G))$ commutes with B and therefore with $C_L(K)$, pointwise. So

$$F(H) = F(I(G)) \cap C_L(K) \subset C_L C_L(K) \cap C_L C_L(K) \cap C_L(K) = C(C_L(K)).$$

The reversed inclusion being obvious, $C_L(k)$ is a Galois extension of $C(C_L(K))$ with H as a Galois group of finite order. By [3, Satz 2], $[L : K] = (G : I(G))$. $[C_L(K) : C(L)]$. Since $C(L) \subseteq C(C_L(K)) \subseteq C_L(K)$ we conclude that $[C_L(K) : C(C_L(K))]$ divides n. Therefore $C_L(K)/C(C_L(K))$ satisfies the second and third assumptions of the theorem. It follows exactly as above that $\# H = [C_L(K) : C(C_L(K))]$. In particular, $\# H$ is a square. Since n satisfies P, the group G has property $P(p_1, \ldots, p_k)$ for certain primes $p_1, \ldots, p_k$, hence so does H, being a factor group of the subgroup $I(G)$ of G, by the lemma. Write

$$\# H = p_1^{2r_1} \ldots p_k^{2r_k}.$$

Take l maximal such that $r_l \neq 0$; $l \geq 1$ since $C_L(K)$ is assumed not to be commutative. Apparently, H has property $P(p_1, \ldots, p_l)$.

If H_1 is the normal p_1 – Sylow group of H, we see, by [3, Hilfsatz 2] that $F(H_1)/C(C_L(k))$ has a Galois group G_1 that is a homomorphic image of H/H_1. Because $[C_L(K) : F(H_1)] \leq \# H_1$, $[F(H_1) : C(C_L(K))] \leq \# G_1 \leq \# H/H_1$ and $[C_L(K) : C(C_L(K))] = \# H$, we must have $G_1 \cong H/H_1$ and

$$[F(H_1) : C(C_L(K))] = \# G_1 = p_2^{2r_2} \ldots p_l^{2r_l}.$$

Repeating this argument we find a field R, $C(C_L(K)) \subset R \subset C_L(K)$, such that $[R : C(C_L(K))] = p_l^{2r_l}$ and $R/C(C_L(K))$ has a Galois group of order $p_l^{2r_l}$. By [3, Satz 4], $R = C_R(C(C_L(K))) = C(R) \cdot C(C_L(K)) = C(R)$. So R is commutative and is therefore contained in a maximal commutative subfield M of $C_L(K)$. But then $[M : C(C_L(K))] = p_1^{r_1} \ldots p_l^{r_l}$. Since $[R : C(C_L(K))] = p_l^{2r_l}$ we conclude that $r_l = 0$, which gives a contradiction.

AN EXAMPLE. To construct a skew field extension L/K satisfying the conditions of the theorem with $K \neq C(L)$, we follow the same method as Albrecht did in [1, p. 1559] to construct a nonregular Galois extension. Take $\mathbb{Q}$-central division algebras K_1, K_2 with $[K_1 : \mathbb{Q}] = 11^2$, $[K_2 : \mathbb{Q}] = 3^2$. This is possible, due to a construction of G. Köthe ([2, p. 23, 24]). Take $L = K_1 \otimes_{\mathbb{Q}} K_2$. Let K be a maximal commutative subfield of K_1. We will show that L/K satisfies the assumptions of the theorem: We have $[L : K] = 11.3^2$, which satisfies P by [1, Bemerkung 7, p. 1556]. Furthermore $C_L(K)$, being equal to $K \otimes_{\mathbb{Q}} K_2$, is not commutative. $C_L(K)$ does not contain a primitive p-th root of unity for any prime number $p \neq 2$, because $\mathbb{Q}$ doesn't and $[C_2(K) : \mathbb{Q}]$ is odd. So theorem 3 applies to L/K.

REFERENCES

1. Albrecht, Uwe – Nicht-streng galoissche Schiefkörpererweiterungen endlichen Ranges über dem Zentrum. Commun. in Algebra, **6**, 1553–1562 (1978).
2. Köthe, Gottfried – Schiefkörper unendlichen Ranges über dem Zentrum. Math. Ann. **105**, 14–39 (1931).
3. Moriya, Mikao – Zur galoisschen Theorie der Schiefkörper. Math. J. Okayama Univ. **9**, 49–62 (1959).